Disclosure of Data Through Website Cookies May Be a Data Breach – What A Recent Court Ruling Means for Healthcare Businesses

Insights
8.13.24

A California federal court recently ruled that disclosure of certain data collected through website cookies that may qualify as health information could trigger a data breach under the California Consumer Privacy Act (CCPA) – a decision that should cause healthcare companies to rethink their data privacy practices. The plaintiff claimed that an online counseling service where website users can find and seek therapy violated the CCPA by allowing tracking software to retarget website users with ads. The court refused to dismiss the CCPA data breach claim because the information being disclosed through retargeting cookies – specifically the fact a user visited the website – may qualify as health information because such a visit could mean they must have been seeking therapy. For healthcare businesses, regardless of whether they are subject to the CCPA, this ruling has significant implications for your website and digital marketing strategy.

What Triggers a Data Breach Under the CCPA?

The CCPA does not provide a private right of action except where a data breach involving certain sensitive information resulted from a covered entity's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information. The unauthorized disclosure of the following types of personal information may be a data breach under the CCPA if the data was unencrypted and unredacted:

- Email address or username and its accompanying password or security question and answer
- Social security number, driver's license, passport number, state identification number, military identification number, tax identification number
- Medical information
- Unique biometric information

To sue for a CCPA data breach, a plaintiff would have to prove that one of these categories of information was disclosed to an unauthorized person and that the disclosure resulted from the business's failure to implement reasonable security measures.

How Does Cookie Retargeting Work?

Cookies are small pieces of information sent from a website you visit to your browser containing information about your activity on that website (i.e., browsing behavior). Third-party cookies are cookies placed on a website by a third party (someone other than the website operator, such as a social media platform or ad tracking company).

Retargeting cookies are specific types of third-party cookies that track and store information about a user's activity on a particular website in order to entice or attract the user (through targeted ad placement) back to the original website when the user browses through other websites. When retargeting cookies are in use, the fact you visited the website and interacted with it may be linked specifically to you through your browser or device and then shared with third parties, and once you go to the websites of those third parties (such as a social media platform), you will see ads from the original website you had visited.

What Happened?

The recent ruling involved users of the website, BetterHelp, and third-party retargeting cookies. BetterHelp is an online platform that connects its users to therapists and therapy-related services. The plaintiffs brought a class action alleging that the company violated the CCPA by sharing the fact that a user had visited the website with third parties through cookies.

The court allowed the CCPA data breach claim to proceed because disclosure of the information those cookies are alleged to have collected could amount to a data breach of the users' medical information. Since the website itself facilitates the provision of healthcare services, a user's interaction with the website could mean they are seeking or receiving medical services. This fact alone may qualify as "medical information" under the CCPA – at least at the motion to dismiss stage, where the court is required to presume that the factual allegations of the complaint are true for purposes of deciding whether the allegations could perhaps establish the claim. The court also reasoned that the claim can proceed because it can reasonably be argued that allowing tracking software on the website "was not an appropriate security procedure or practice, given the nature of the information."

The court did not make any rulings on whether such use of retargeting cookies definitively constitutes a CCPA violation and whether having such technology on a website is definitively not an appropriate security measure (only that it could be for purposes of a motion to dismiss). However, by allowing the CCPA claim to proceed, this signals that the disclosure of CCPA-protected data through cookies could constitute a data breach. It is worth noting that the court's ruling still leaves open the question of whether the website users had adequately consented to the recording of such information and, if so, whether that consent will defeat the claim.

This ruling has the potential of providing fodder to claims against healthcare-related websites outside the CCPA context, as California law (and the laws of every single state in the US) includes medical information among the types of information that trigger a reportable data breach. Does the

fact that a person visited the website of a provider of healthcare services itself qualify as medical information? This could be the next battleground.

Your Next Steps

Here are some ways that healthcare entities can avoid being targeted for potential data breach class actions based on your website use of cookies:

1. Familiarize Yourself with Applicable Law: Ensure you have a thorough understanding of the CCPA and other applicable laws, including when the disclosure of certain types of data constitutes a data breach. Seek legal advice from your privacy counsel on whether a user's interaction with your website results in collection or disclosure of data that may qualify as medical information.

2. Cookie Consent Banners: While the court did not rule on the issue of consent, consent can help protect against a data breach claim. Use cookie consent banners or pop-ups that require users to opt-in before any non-essential cookies, including third-party retargeting cookies, are placed on their devices or browsers.

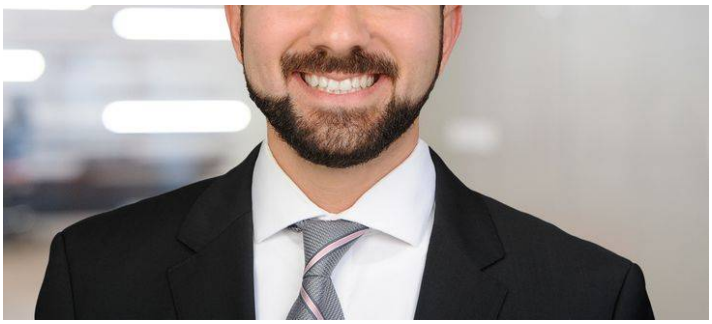
3. Arbitration Agreements: One potential way to manage the legal risk is to include in your website Terms of Use an arbitration provision with a class action waiver. But make sure you engage legal counsel for this, as it's not just about having the right language in the agreement but also how it is presented and how you can prove that a website user agreed to arbitration and a class action waiver.

4. Stay on Top of Changes: State data privacy laws are constantly changing and being interpreted and applied in new ways. Staying updated on developments such as these is important to remain compliant with obligations under the CCPA and other applicable state laws.

Conclusion

Consumer privacy laws are an ever-developing and ever-evolving area. The best strategy to stay compliant is to continue evaluating your data collecting processes and security measures and adjust them depending on new rulings or interpretations. Make sure that you are subscribed to Fisher Phillips' Insights to get the most up-to-date information direct to your inbox. For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's Consumer Privacy Team or Healthcare Industry Team.

Related People



Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Rachel Song
Associate
415.926.7651

Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Litigation and Trials

Industry Focus

Healthcare

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

San Francisco

Woodland Hills